



C

configuration files

- archiving [2-12](#)
- clearing the startup configuration [2-12](#)
- creating and using, guidelines for [2-2](#)
- creating using a text editor [2-2](#)
- deleting a stored configuration [2-12](#)
- described [2-1](#)
- downloading
 - reasons for [2-1](#)
 - using FTP [2-6](#)
 - using RCP [2-10](#)
 - using TFTP [2-3](#)
- invalid combinations when copying [1-6](#)
- replacing and rolling back, guidelines for [2-13](#)
- replacing a running configuration [2-12, 2-13](#)
- rolling back a running configuration [2-12, 2-13](#)
- uploading
 - reasons for [2-2](#)
 - using FTP [2-7](#)
 - using RCP [2-11](#)
 - using TFTP [2-4](#)
- configuration replacement [2-12](#)
- configuration rollback [2-12](#)

D

directories

- changing [1-4](#)
- creating and removing [1-5](#)
- displaying the working [1-4](#)
- downloading

configuration files

- reasons for [2-1](#)
- using FTP [2-6](#)
- using RCP [2-10](#)
- using TFTP [2-3](#)

image files

- deleting old image [3-4](#)
- preparing [3-3, 3-6, 3-11](#)
- reasons for [3-1](#)
- using FTP [3-7](#)
- using HTTP [3-1](#)
- using RCP [3-12](#)
- using TFTP [3-3](#)
- using the Device Manager [3-1](#)

F

files

- copying [1-6](#)
- deleting [1-6](#)
- displaying the contents of [1-8](#)
- tar
 - creating [1-7](#)
 - displaying the contents of [1-7](#)
 - extracting [1-8](#)
 - image file format [3-2](#)

file system

- displaying available file systems [1-1](#)
- displaying file information [1-4](#)
- local file system names [1-1](#)
- network file system names [1-6](#)
- setting the default [1-3](#)
- flash device, number of [1-1](#)

FTP

- configuration files
 - downloading [2-6](#)
 - overview [2-5](#)
 - uploading [2-7](#)
- image files
 - deleting old image [3-9](#)
 - downloading [3-7](#)
 - preparing the server [3-6](#)
 - uploading [3-9](#)

- clearing [2-12](#)

N

Network Assistant

- upgrading a switch [3-1](#)

R

RCP

- configuration files
 - downloading [2-10](#)
 - overview [2-8](#)
 - uploading [2-11](#)
- image files
 - deleting old image [3-13](#)
 - downloading [3-12](#)
 - preparing the server [3-11](#)
 - uploading [3-13](#)

running configuration

- replacing [2-12, 2-13](#)
- rolling back [2-12, 2-13](#)

S

software images

- location in flash [3-2](#)
- tar file format, described [3-2](#)

startup configuration

T

tar files

- creating [1-7](#)
- displaying the contents of [1-7](#)
- extracting [1-8](#)
- image file format [3-2](#)

TFTP

- configuration files
 - downloading [2-3](#)
 - uploading [2-4](#)
- image files
 - deleting [3-4](#)
 - downloading [3-3](#)
 - preparing the server [3-3](#)
 - uploading [3-5](#)

U

upgrading software images

- See downloading

uploading

- configuration files
 - reasons for [2-2](#)
 - using FTP [2-7](#)
 - using RCP [2-11](#)
 - using TFTP [2-4](#)
- image files
 - preparing [3-3, 3-6, 3-11](#)
 - reasons for [3-1](#)
 - using FTP [3-9](#)
 - using RCP [3-13](#)
 - using TFTP [3-5](#)



Preface

- [Obtaining Documentation and Submitting a Service Request](#), page iii
- [Conventions](#), page iii
- [Related Documentation](#), page iv

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in bold font .
<i>italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
[]	Elements in square brackets are optional.
{ x y z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
<code>courier font</code>	Terminal sessions and information the system displays appear in <code>courier font</code> .
< >	Nonprinting characters such as passwords are in angle brackets.

[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.



Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.



Tip

Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.



Caution

Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.



Timesaver

Means *the described action saves time*. You can save time by performing the action described in the paragraph.



Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS



Warning

Statements using this symbol are provided for additional information and to comply with regulatory and customer requirements.

Related Documentation



Note

Before installing or upgrading the switch, refer to the release notes.

- Catalyst 2960-XR Switch, located at http://www.cisco.com/go/cat2960xr_docs.
- Cisco SFP and SFP+ modules documentation, including compatibility matrixes, located at: http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html



Working with the Flash File System

- [Information About the Flash File System, page 1-1](#)
- [Displaying Available File Systems, page 1-1](#)
- [Setting the Default File System, page 1-3](#)
- [Displaying Information About Files on a File System, page 1-4](#)
- [Changing Directories and Displaying the Working Directory, page 1-4](#)
- [Creating and Removing Directories, page 1-5](#)
- [Copying Files, page 1-6](#)
- [Creating, Displaying, and Extracting Files, page 1-7](#)

Information About the Flash File System

The flash file system is a single flash device on which you can store files. It also provides several commands to help you manage software bundles and configuration files. The default flash file system on the switch is named flash:.

As viewed from the stack master, or any stack member, flash: refers to the local flash device, which is the device attached to the same switch on which the file system is being viewed. In a switch stack, each of the flash devices from the various stack members can be viewed from the stack master. The names of these flash file systems include the corresponding switch member numbers. For example, flash-3:, as viewed from the stack master, refers to the same file system as does flash: on stack member 3. Use the **show file systems** privileged EXEC command to list all file systems, including the flash file systems in the switch stack.

Only one user at a time can manage the software bundles and configuration files for a switch stack.

Displaying Available File Systems

To display the available file systems on your switch, use the **show file systems** privileged EXEC command as shown in this example for a standalone switch:

```
Switch# show file systems
File Systems:
      Size(b)      Free(b)      Type  Flags  Prefixes
*  15998976      5135872      flash  rw     flash:
      -           -           opaque rw     bs:
      -           -           opaque rw     vb:
```

■ Displaying Available File Systems

```

524288      520138      nvram      rw      nvram:
-           -          network     rw      tftp:
-           -          opaque      rw      null:
-           -          opaque      rw      system:
-           -          opaque      ro      xmodem:
-           -          opaque      ro      ymodem:

```

This example shows a switch stack. In this example, the stack master is stack member 1; the file system on stack member 2 is displayed as flash-2, the file system on stack member 3 is displayed as flash-3 and so on. The example also shows the crashinfo directories and a USB flash drive plugged into the stack master.

Switch# **show file systems**

File Systems:

	Size(b)	Free(b)	Type	Flags	Prefixes
	145898496	68792320	disk	rw	crashinfo:
	146014208	99090432	disk	rw	crashinfo-2:
	248512512	87031808	disk	rw	crashinfo-3:
	146276352	108003328	disk	rw	crashinfo-4:
*	1749458944	1258868736	disk	rw	flash:
	729546752	282853376	disk	rw	flash-2:
	1622147072	1173880832	disk	rw	flash-3:
	1749549056	1301282816	disk	rw	flash-4:
	0	0	disk	rw	unix:
	-	-	disk	rw	usbflash0:
	1027342336	64749568	disk	rw	usbflash0-2:
	-	-	disk	rw	usbflash0-3:
	-	-	disk	rw	usbflash0-4:
	-	-	opaque	rw	system:
	-	-	opaque	rw	tmpsys:
	-	-	nvram	rw	stby-nvram:
	-	-	nvram	rw	stby-rcsf:
	-	-	opaque	rw	null:
	-	-	opaque	ro	tar:
	-	-	network	rw	tftp:
	2097152	2071500	nvram	rw	nvram:
	-	-	opaque	wo	syslog:
	-	-	network	rw	rcp:
	-	-	network	rw	http:
	-	-	network	rw	ftp:
	-	-	network	rw	scp:
	-	-	network	rw	https:
	-	-	opaque	ro	cns:

Table 1-1 *show file systems Field Descriptions*

Field	Value
Size(b)	Amount of memory in the file system in bytes.
Free(b)	Amount of free memory in the file system in bytes.

Table 1-1 *show file systems Field Descriptions (continued)*

Field	Value
Type	<p>Type of file system.</p> <p>disk—The file system is for a flash memory device, USB flash, and crashinfo file.</p> <p>network—The file system for network devices; for example, an FTP server or and HTTP server.</p> <p>nvram—The file system is for a NVRAM device.</p> <p>opaque—The file system is a locally generated <i>pseudo</i> file system (for example, the <i>system</i>) or a download interface, such as brimux.</p> <p>unknown—The file system is an unknown type.</p>
Flags	<p>Permission for file system.</p> <p>ro—read-only.</p> <p>rw—read/write.</p> <p>wo—write-only.</p>
Prefixes	<p>Alias for file system.</p> <p>crashinfo:—Crashinfo file.</p> <p>flash:—Flash file system.</p> <p>ftp:—FTP server.</p> <p>http:—HTTP server.</p> <p>https:—Secure HTTP server.</p> <p>nvram:—NVRAM.</p> <p>null:—Null destination for copies. You can copy a remote file to null to find its size.</p> <p>rcp:—Remote Copy Protocol (RCP) server.</p> <p>scp:—Session Control Protocol (SCP) server.</p> <p>system:—Contains the system memory, including the running configuration.</p> <p>tftp:—TFTP network server.</p> <p>xmodem:—Obtain the file from a network machine by using the Xmodem protocol.</p> <p>ymodem:—Obtain the file from a network machine by using the Ymodem protocol.</p>

Setting the Default File System

You can specify the file system or directory that the system uses as the default file system by using the **cd filesystem:** privileged EXEC command. You can set the default file system to omit the *filesystem:* argument from related commands. For example, for all privileged EXEC commands that have the optional *filesystem:* argument, the system uses the file system specified by the **cd** command.

By default, the default file system is *flash:*.

You can display the current default file system as specified by the **cd** command by using the **pwd** privileged EXEC command.

Displaying Information About Files on a File System

You can view a list of the contents of a file system before manipulating its contents. For example, before copying a new configuration file to flash memory, you might want to verify that the file system does not already contain a configuration file with the same name. Similarly, before copying a flash configuration file to another location, you might want to verify its filename for use in another command.

To display information about files on a file system, use one of the privileged EXEC commands listed in [Table 1-2](#).

Table 1-2 Commands for Displaying Information About Files

Command	Description
dir [/all] [filesystem:][filename]	Displays a list of files on a file system.
show file systems	Displays more information about each of the files on a file system.
show file information file-url	Displays information about a specific file.
show file descriptors	Displays a list of open file descriptors. File descriptors are the internal representations of open files. You can use this command to see if another user has a file open.

To display information about the driver text object in the CISCO-MEMORY-POOL-MIB, use the **show memory** privileged EXEC command:

```
Switch# show memory
System memory   : 1939252K total, 1317664K used, 621588K free, 118580K kernel reserved
Lowest (b)      : 54189544

                Total (K)    Used (K)    Free (K)
Process        1939252      1317664      621588
Config         0            0            0
```

Changing Directories and Displaying the Working Directory

Beginning in privileged EXEC mode, follow these steps to change directories and to display the working directory:

	Command	Purpose
Step 1	dir filesystem:	Displays the directories on the specified file system. For <i>filesystem:</i> , use <i>flash:</i> for the system board flash device.
	Example: Switch# dir flash:	To access flash partitions of switch members in a stack, use <i>flash-n</i> where <i>n</i> is the stack member number. For example, <i>flash-4</i> .
Step 2	cd directory_name	Navigates to the specified directory. The command example shows how to navigate to the directory named <i>new_configs</i> .
	Example: Switch# cd new_configs	

	Command	Purpose
Step 3	pwd Example: Switch# pwd	Displays the working directory.
Step 4	cd Example: Switch# cd	Navigates to the default directory.

Creating and Removing Directories

Beginning in privileged EXEC mode, follow these steps to create a directory:

	Command	Purpose
Step 1	dir filesystem: Example: Switch# dir flash:	Displays the directories on the specified file system. For <i>filesystem:</i> , use flash: for the system board flash device.
Step 2	mkdir directory_name Example: Switch# mkdir old_configs	Creates a new directory. Directory names are case sensitive and are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, slashes, quotes, semicolons, or colons.
Step 3	dir filesystem: Example: Switch# dir flash:	Verifies your entry.

To remove a directory with all its files and subdirectories, use the **delete /force /recursive filesystem:/file-url** privileged EXEC command.

Use the **/recursive** keyword to delete the named directory and all subdirectories and the files contained in it. Use the **/force** keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process.

For *filesystem*, use **flash:** for the system board flash device. For *file-url*, enter the name of the directory to be deleted. All the files in the directory and the directory are removed.



Caution

When files and directories are deleted, their contents cannot be recovered.

Copying Files

To copy a file from a source to a destination, use the **copy** *source-url destination-url* privileged EXEC command. For the source and destination URLs, you can use **running-config** and **startup-config** keyword shortcuts. For example, the **copy running-config startup-config** command saves the currently running configuration file to the NVRAM section of flash memory to be used as the configuration during system initialization.

You can also copy from special file systems (**xmodem:**, **ymodem:**) as the source for the file from a network machine that uses the Xmodem or Ymodem protocol.

Network file system URLs include **ftp:**, **rcp:**, and **tftp:** and have these syntaxes:

- FTP—**ftp:**[[//username [:password]@location]/directory]/filename
- RCP—**rcp:**[[//username@location]/directory]/filename
- TFTP—**tftp:**[[//location]/directory]/filename

Local writable file systems include flash:.

Some invalid combinations of source and destination exist. Specifically, you cannot copy these combinations:

- From a running configuration to a running configuration
- From a startup configuration to a startup configuration
- From a device to the same device (for example, the **copy flash: flash:** command is invalid)

For specific examples of using the **copy** command with configuration files, see the [Chapter 2, “Working with the Configuration Files.”](#)

Deleting Files

When you no longer need a file on a flash memory device, you can permanently delete it. To delete a file or directory from a specified flash device, use the **delete** [/force] [/recursive] [filesystem:] /file-url privileged EXEC command.

Use the **/recursive** keyword for deleting a directory and all subdirectories and the files contained in it. Use the **/force** keyword to suppress the prompting that confirms a deletion of each file in the directory. You are prompted only once at the beginning of this deletion process. Use the **/force** and **/recursive** keywords for deleting old software images that were installed by using the **archive download-sw** command but are no longer needed.

If you omit the *filesystem:* option, the switch uses the default device specified by the **cd** command. For *file-url*, you specify the path (directory) and the name of the file to be deleted.

When you attempt to delete any files, the system prompts you to confirm the deletion.

**Caution**

When files are deleted, their contents cannot be recovered.

This example shows how to delete the file *myconfig* from the default flash memory device:

```
Switch# delete myconfig
```

Creating, Displaying, and Extracting Files

You can create a file and write files into it, list the files in a file, and extract the files from a file as described in the next sections.

Beginning in privileged EXEC mode, follow these steps to create a file, display the contents, and extract it:

Command	Purpose
Step 1 archive tar /create <i>destination-url flash:/file-url</i> Example: <pre>Switch# archive tar /create tftp:172.20.10.30/saved. flash:/new-configs</pre>	<p>Creates a file and adds files to it.</p> <p>For <i>destination-url</i>, specify the destination URL alias for the local or network file system and the name of the file to create. The <i>-filename</i>, is the file to be created. These options are supported:</p> <ul style="list-style-type: none"> Local flash file system syntax: flash: FTP syntax: ftp:[[/username[:password]@location]/directory]/-filename. RCP syntax: rcp:[[/username@location]/directory]/-filename. TFTP syntax: tftp:[[/location]/directory]/-filename. <p>For flash:/file-url, specify the location on the local flash file system in which the new file is created. You can also specify an optional list of files or directories within the source directory to add to the new file. If none are specified, all files and directories at this level are written to the newly created file.</p>
Step 2 archive tar /table <i>source-url</i> Example: <pre>Switch# archive tar /table flash:/new-configs</pre>	<p>Displays the contents of a file.</p> <p>For <i>source-url</i>, specify the source URL alias for the local or network file system. The <i>-filename</i>, is the file to display. These options are supported:</p> <ul style="list-style-type: none"> Local flash file system syntax: flash: FTP syntax: ftp:[[/username[:password]@location]/directory]/-filename. RCP syntax: rcp:[[/username@location]/directory]/-filename. TFTP syntax: tftp:[[/location]/directory]/-filename. <p>You can also limit the file displays by specifying a list of files or directories after the file. Only those files appear. If none are specified, all files and directories appear.</p>

	Command	Purpose
Step 3	archive tar /xtract <i>source-url</i> <i>flash:/file-url</i> [<i>dir/file...</i>] Example: Switch# archive tar /xtract tftp:/172.20.10.30/saved. flash:/new-configs	<p>Extracts a file into a directory on the flash file system.</p> <p>For <i>source-url</i>, specify the source URL alias for the local file system. The <i>-filename.</i> is the file from which to extract files. These options are supported:</p> <ul style="list-style-type: none"> local flash file system syntax: flash: FTP syntax: ftp:[[/username[:password]@location]/directory]/-filename. RCP syntax: rcp:[[/username@location]/directory]/-filename. TFTP syntax: tftp:[[/location]/directory]/-filename. <p>For flash:/file-url [<i>dir/file...</i>], specify the location on the local flash file system from which the file is extracted. Use the <i>dir/file...</i> option to specify a list of files or directories within the file to be extracted. If none are specified, all files and directories are extracted.</p>
Step 4	more [/ascii /binary /ebcdic] <i>file-url</i> Example: Switch# more flash: /new-configs	<p>Displays the contents of any readable file, including a file on a remote file system.</p>

This example shows how to create a file. This command writes the contents of the *new-configs* directory on the local flash device to a file named *saved.* on the TFTP server at 172.20.10.30:

```
Switch# archive tar /create tftp:172.20.10.30/saved. flash:/new-configs
```

This example shows how to extract the contents of a file located on the TFTP server at 172.20.10.30:

```
Switch# archive tar /xtract tftp:/172.20.10.30/saved. flash:/new-configs
```



Working with the Configuration Files

- [Information About Configuration Files, page 2-1](#)
- [Guidelines for Creating and Using Configuration Files, page 2-2](#)
- [Creating a Configuration File Using a Text Editor, page 2-2](#)
- [Copying Configuration Files Using TFTP, page 2-3](#)
- [Copying Configuration Files Using FTP, page 2-5](#)
- [Copying Configuration Files Using RCP, page 2-8](#)
- [Clearing Configuration Information, page 2-11](#)
- [Replacing and Rolling Back Configurations, page 2-12](#)

Information About Configuration Files

Configuration files contain commands that you enter to customize the function of the Cisco IOS software. You can create a basic configuration file by using the **setup** program or by entering the **setup** privileged EXEC command.

Startup configuration files are used during system startup to configure the software. Running configuration files contain the current configuration of the software. The two configuration files can be different. The startup configuration is stored in the NVRAM section of flash memory and is persistent; the running configuration is stored in DRAM and is replaced by the startup configuration at the next reboot.

You can copy (*download*) configuration files from a TFTP, FTP, or RCP server to the running configuration or startup configuration of the switch. You perform this task when you want to:

- Restore a backed-up configuration file.
- Use the configuration file for another switch.

For example, you might add another switch to your network and want it to have a configuration similar to the original switch. By copying the file to the new switch, you can change the relevant parts rather than recreating the whole file.

- Load the same configuration commands on all the switches in your network so that all the switches have similar configurations.

The **copy {ftp: | rcp: | tftp:} system:running-config** privileged EXEC command loads the configuration files on the switch as if you were entering the commands at the command line. The switch does not erase the existing running configuration before adding the commands. If a command in the copied configuration file replaces a command in the existing configuration file, the existing command is

erased. For example, if the copied configuration file contains a different IP address in a particular command than the existing configuration, the IP address in the copied configuration is used. However, some commands in the existing configuration might not be replaced or negated. In this case, the resulting configuration file is a mixture of the existing configuration file and the copied configuration file, with the copied configuration file having precedence. To restore a configuration file to an exact copy of a file stored on a server, copy the configuration file directly to the startup configuration (by using the **copy {ftp: | rcp: | tftp:} nvram:startup-config** privileged EXEC command), and reload the switch.

You can copy (*upload*) configuration files from the switch to a file server by using TFTP, FTP, or RCP. You might perform this task to back up a current configuration file to a server before changing its contents so that you can later restore the original configuration file from the server.

Guidelines for Creating and Using Configuration Files

Creating configuration files can aid in your switch configuration. Configuration files can contain some or all of the commands needed to configure one or more switches. For example, you might want to download the same configuration file to several switches that have the same hardware configuration.

Use these guidelines when creating a configuration file:

- We recommend that you connect through the console port or Ethernet management port for the initial configuration of the switch. If you are accessing the switch through a network connection instead of through a direct connection to the console port or Ethernet management port, keep in mind that some configuration changes (such as changing the switch IP address or disabling ports) can cause a loss of connectivity to the switch.
- If no password has been set on the switch, we recommend that you set one by using the **enable secret secret-password** global configuration command.

Creating a Configuration File Using a Text Editor

When creating a configuration file, you must list commands logically so that the system can respond appropriately. To create a configuration file using a text editor, follow these steps:

-
- | | |
|---------------|---|
| Step 1 | Copy an existing configuration from a switch to a server.

For more information, see the “Downloading the Configuration File Using TFTP” section on page 2-3, the “Downloading a Configuration File Using FTP” section on page 2-6, or the “Downloading a Configuration File Using RCP” section on page 2-10. |
| Step 2 | Open the configuration file in a text editor, such as vi or emacs on UNIX or Notepad on a PC. |
| Step 3 | Extract the portion of the configuration file with the desired commands, and save it in a new file. |
| Step 4 | Copy the configuration file to the appropriate server location. For example, copy the file to the TFTP directory on the workstation (usually /tftpboot on a UNIX workstation). |
| Step 5 | Make sure the permissions on the file are set to world-read. |
-

Copying Configuration Files Using TFTP

You can configure the switch with configuration files that you create from scratch, download from another switch, or download from a TFTP server. You can copy (upload) configuration files to a TFTP server for storage.

- [Preparing to Download or Upload a Configuration File Using TFTP, page 2-3](#)
- [Downloading the Configuration File Using TFTP, page 2-3](#)
- [Uploading the Configuration File Using TFTP, page 2-4](#)

Preparing to Download or Upload a Configuration File Using TFTP

- Ensure that the workstation acting as the TFTP server is properly configured. On a Sun workstation, make sure that the `/etc/inetd.conf` file contains this line:

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
```

Make sure that the `/etc/services` file contains this line:

```
tftp 69/udp
```



Note You must restart the `inetd` daemon after modifying the `/etc/inetd.conf` and `/etc/services` files. To restart the daemon, either stop the `inetd` process and restart it, or enter a **fastboot** command (on the SunOS 4.x) or a **reboot** command (on Solaris 2.x or SunOS 5.x). For more information on the TFTP daemon, see the documentation for your workstation.

- Ensure that the switch has a route to the TFTP server. The switch and the TFTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server by using the **ping** command.
- Ensure that the configuration file to be downloaded is in the correct directory on the TFTP server (usually `/tftpboot` on a UNIX workstation).
- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-read.
- Before uploading the configuration file, you might need to create an empty file on the TFTP server. To create an empty file, enter the **touch filename** command, where *filename* is the name of the file you will use when uploading it to the server.
- During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) on the server, ensure that the permissions on the file are set correctly. Permissions on the file should be world-write.

Downloading the Configuration File Using TFTP

To configure the switch by using a configuration file downloaded from a TFTP server, follow these steps:

- Step 1** Copy the configuration file to the appropriate TFTP directory on the TFTP server.
- Step 2** Verify that the TFTP server is properly configured by referring to the [“Preparing to Download or Upload a Configuration File Using TFTP”](#) section on page 2-3.

Step 3 Log into the switch through the console port, the Ethernet management port, or a Telnet session.

Step 4 Download the configuration file from the TFTP server to configure the switch.

Specify the IP address or hostname of the TFTP server and the name of the file to download.

Use one of these privileged EXEC commands:

- **copy tftp:[[/location]/directory]/filename system:running-config**
- **copy tftp:[[/location]/directory]/filename nvram:startup-config**
- **copy tftp:[[/location]/directory]/filename flash-[n]:/directory/startup-config**

The configuration file downloads, and the commands are executed as the file is parsed line-by-line.

This example shows how to configure the software from the file *tokyo-config* at IP address 172.16.2.155:

```
Switch# copy tftp://172.16.2.155/tokyo-config system:running-config
Configure using tokyo-config from 172.16.2.155? [confirm] y
Booting tokyo-config from 172.16.2.155:!!! [OK - 874/16000 bytes]
```

Uploading the Configuration File Using TFTP

To upload a configuration file from a switch to a TFTP server for storage, follow these steps:

Step 1 Verify that the TFTP server is properly configured by referring to the [“Preparing to Download or Upload a Configuration File Using TFTP” section on page 2-3](#).

Step 2 Log into the switch through the console port, the Ethernet management port, or a Telnet session.

Step 3 Upload the switch configuration to the TFTP server. Specify the IP address or hostname of the TFTP server and the destination filename.

Use one of these privileged EXEC commands:

- **copy system:running-config tftp:[[/location]/directory]/filename**
- **copy nvram:startup-config tftp:[[/location]/directory]/filename**
- **copy flash-[n]:/directory/startup-config tftp:[[/location]/directory]/filename**

The file is uploaded to the TFTP server.

This example shows how to upload a configuration file from a switch to a TFTP server:

```
Switch# copy system:running-config tftp://172.16.2.155/tokyo-config
Write file tokyo-config on host 172.16.2.155? [confirm] y
#
Writing tokyo-config!!! [OK]
```


Copying Configuration Files Using FTP

You can copy configuration files to or from an FTP server.

- [Preparing to Download or Upload a Configuration File Using FTP, page 2-5](#)
- [Downloading a Configuration File Using FTP, page 2-6](#)
- [Uploading a Configuration File Using FTP, page 2-7](#)

Preparing to Download or Upload a Configuration File Using FTP

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy a configuration file from the switch to a server by using FTP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **copy** command if a username is specified.
- The username set by the **ip ftp username** *username* global configuration command if the command is configured.
- Anonymous.

The switch sends the first valid password in this list:

- The password specified in the **copy** command if a password is specified.
- The password set by the **ip ftp password** *password* global configuration command if the command is configured.
- The switch forms a password named *username@switchname.domain*. The variable *username* is the username associated with the current session, *switchname* is the configured hostname, and *domain* is the domain of the switch.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept your FTP write request.

Use the **ip ftp username** and **ip ftp password** commands to specify a username and password for all copies. Include the username in the **copy** command if you want to specify only a username for that copy operation.

If the server has a directory structure, the configuration file is written to or copied from the directory associated with the username on the server. For example, if the configuration file resides in the home directory of a user on the server, specify that user's name as the remote username.

Before you begin downloading or uploading a configuration file, do the following:

- Ensure that the switch has a route to the FTP server. The switch and the FTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the FTP server by using the **ping** command.
- If you are accessing the switch through the console or a Telnet session and you do not have a valid username, make sure that the current FTP username is the one that you want to use for the FTP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new FTP username by using the **ip ftp username** *username* global configuration command during all copy operations. The new username is stored in NVRAM. If you are accessing the switch through a Telnet session and you have a valid username, this username is used, and you do not need to set the FTP username. Include the username in the **copy** command if you want to specify a username for only that copy operation.

- When you upload a configuration file to the FTP server, it must be properly configured to accept the write request from the user on the switch.

For more information, see the documentation for your FTP server.

Downloading a Configuration File Using FTP

Beginning in privileged EXEC mode, follow these steps to download a configuration file by using FTP:

	Command	Purpose
Step 1	configure terminal Example: Switch# configure terminal	(Optional) Enters global configuration mode on the switch. This step is required only if you override the default remote username or password.
Step 2	ip ftp username <i>username</i> Example: Switch(config)# ip ftp username NetAdmin1	(Optional) Changes the default remote FTP username.
Step 3	ip ftp password <i>password</i> Example: Switch(config)# ip ftp password adminpassword	(Optional) Changes the default FTP password.
Step 4	end Example: Switch(config)# end	Returns to privileged EXEC mode.
Step 5	copy ftp:[[/[<i>username</i>[:<i>password</i>]@]<i>location</i>]/<i>directory</i>]/<i>filename</i>] system:running-config or copy ftp:[[/[<i>username</i>[:<i>password</i>]@]<i>location</i>]/<i>directory</i>]/<i>filename</i>] nvram:startup-config Example: Switch# copy ftp system:running-config	Copies the configuration file from the FTP server to the running configuration or to the startup configuration file.

This example shows how to copy a configuration file named *host1-config* from the home directory for user *netadmin1* on the remote server with an IP address of 172.16.101.101 and to load and run those commands on the switch:

```
Switch# copy ftp://netadmin1:mypass@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-config:![OK]
Switch#
%SYS-5-CONFIG: Configured from host1-config by ftp from 172.16.101.101
```

This example shows how to specify a remote username of *netadmin1*. The software copies the configuration file *host2-confg* from the home directory for user *netadmin1* on the remote server with an IP address of 172.16.101.101 to the switch startup configuration.

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin1
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy ftp: nvram:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-confg]? host2-confg
Configure using host2-confg from 172.16.101.101?[confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-confg:[OK]
[OK]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-confg by ftp from
172.16.101.101
```

Uploading a Configuration File Using FTP

Beginning in privileged EXEC mode, follow these steps to upload a configuration file by using FTP:

	Command	Purpose
Step 1	configure terminal Example: Switch# configure terminal	(Optional) Enters global configuration mode. This step is required only if you override the default remote username or password.
Step 2	ip ftp username <i>username</i> Example: Switch(config)# ip ftp username NetAdmin1	(Optional) Changes the default remote username.
Step 3	ip ftp password <i>password</i> Example: Switch(config)# ip ftp password adminpassword	(Optional) Changes the default password.

	Command	Purpose
Step 4	end Example: Switch(config)# end	Returns to privileged EXEC mode.
Step 5	copy system:running-config ftp:[[/[[[username[:password]@]location]/directory] /filename] or copy nvram:startup-config ftp:[[/[[[username[:password]@]location]/directory] /filename] Example: Switch# copy system:running-config ftp:	Copies the specified configuration file to the specified location on the FTP server.

This example shows how to copy the running configuration file named *switch2-config* to the *netadmin1* directory on the remote host with an IP address of 172.16.101.101:

```
Switch# copy system:running-config ftp://netadmin1:mypass@172.16.101.101/switch2-config
Write file switch2-config on host 172.16.101.101? [confirm]
Building configuration... [OK]
Connected to 172.16.101.101
Switch#
```

This example shows how to store a startup configuration file on a server by using FTP to copy the file:

```
Switch# configure terminal
Switch(config)# ip ftp username netadmin2
Switch(config)# ip ftp password mypass
Switch(config)# end
Switch# copy nvram:startup-config ftp:
Remote host[]? 172.16.101.101
Name of configuration file to write [switch2-config]?
Write file switch2-config on host 172.16.101.101? [confirm]
! [OK]
```

Copying Configuration Files Using RCP

You can copy configuration files from and to an RCP server.

- [Preparing to Download or Upload a Configuration File Using RCP, page 2-8](#)
- [Downloading a Configuration File Using RCP, page 2-10](#)
- [Uploading a Configuration File Using RCP, page 2-11](#)

Preparing to Download or Upload a Configuration File Using RCP

To copy configuration files using RCP, you need access to a server that supports the remote shell (rsh). (Most UNIX systems support rsh.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, RCP creates it for you.

RCP requires a client to send a remote username with each RCP request to a server. When you copy a configuration file from the switch to a server, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **copy** command if a username is specified.
- The username set by the **ip rcmd remote-username username** global configuration command if the command is configured.
- The remote username associated with the current TTY (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** command, the switch software sends the Telnet username as the remote username.
- The switch hostname.

For a successful RCP copy request, you must define an account on the network server for the remote username. If the server has a directory structure, the configuration file is written to or copied from the directory associated with the remote username on the server. For example, if the configuration file is in the home directory of a user on the server, specify that user's name as the remote username.

Before you begin downloading or uploading a configuration file by using RCP, do the following:

- Ensure that the workstation acting as the RCP server supports the remote shell (rsh).
- Ensure that the switch has a route to the RCP server. The switch and the server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the RCP server by using the **ping** command.
- If you are accessing the switch through the console or a Telnet session and you do not have a valid username, make sure that the current RCP username is the one that you want to use for the RCP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new RCP username by using the **ip rcmd remote-username username** global configuration command to be used during all copy operations. The new username is stored in NVRAM. If you are accessing the switch through a Telnet session and you have a valid username, this username is used, and you do not need to set the RCP username. Include the username in the **copy** command if you want to specify a username for only that copy operation.
- When you upload a file to the RCP server, it must be properly configured to accept the RCP write request from the user on the switch. For UNIX systems, you must add an entry to the **.rhosts** file for the remote user on the RCP server. For example, suppose that the switch contains these configuration lines:

```
hostname Switch1
ip rcmd remote-username User0
```

If the switch IP address translates to *Switch1.company.com*, the **.rhosts** file for User0 on the RCP server should contain this line:

```
Switch1.company.com Switch1
```

For more information, see the documentation for your RCP server.

Downloading a Configuration File Using RCP

Beginning in privileged EXEC mode, follow these steps to download a configuration file by using RCP:

	Command	Purpose
Step 1	configure terminal Example: Switch# <code>configure terminal</code>	(Optional) Enters global configuration mode. This step is required only if you override the default remote username.
Step 2	ip rcmd remote-username <i>username</i> Example: Switch(config)# <code>ip rcmd remote-username netadmin1</code>	(Optional) Specifies the remote username.
Step 3	end Example: Switch(config)# <code>end</code>	Returns to privileged EXEC mode.
Step 4	copy rcp:[[/[<i>username</i>@]<i>location</i>]/<i>directory</i>]/<i>filename</i>] system:running-config or copy rcp:[[/[<i>username</i>@]<i>location</i>]/<i>directory</i>]/<i>filename</i>] nvrn:startup-config Example: Switch# <code>copy rcp: system:running-config</code>	Using RCP, copies the configuration file from a network server to the running configuration or to the startup configuration file.

This example shows how to copy a configuration file named *host1-config* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 and load and run those commands on the switch:

```
Switch# copy rcp://netadmin1@172.16.101.101/host1-config system:running-config
Configure using host1-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host1-config:![OK]
Switch#
%SYS-5-CONFIG: Configured from host1-config by rcp from 172.16.101.101
```

This example shows how to specify a remote username of *netadmin1* and copy the configuration file *host2-config* from the *netadmin1* directory on the remote server with an IP address of 172.16.101.101 to the startup configuration:

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin1
Switch(config)# end
Switch# copy rcp: nvrn:startup-config
Address of remote host [255.255.255.255]? 172.16.101.101
Name of configuration file[rtr2-config]? host2-config
Configure using host2-config from 172.16.101.101? [confirm]
Connected to 172.16.101.101
Loading 1112 byte file host2-config:![OK]
[OK]
Switch#
%SYS-5-CONFIG_NV:Non-volatile store configured from host2-config by rcp from
172.16.101.101
```

Uploading a Configuration File Using RCP

Beginning in privileged EXEC mode, follow these steps to upload a configuration file by using RCP:

	Command	Purpose
Step 1	configure terminal Example: Switch# configure terminal	(Optional) Enters global configuration mode. This step is required only if you override the default remote username.
Step 2	ip rcmd remote-username username Example: Switch(config)# ip rcmd remote-username netadmin1	(Optional) Specifies the remote username.
Step 3	end Example: Switch(config)# end	Returns to privileged EXEC mode.
Step 4	copy system:running-config rcp:[[/[username@]location]/directory]/filename] or copy nvram:startup-config rcp:[[/[username@]location]/directory]/filename] Example: Switch# copy system:running-config rcp:	Using RCP, copies the specified configuration file from the switch running to the specified network server.

This example shows how to copy the running configuration file named *switch2-config* to the *netadmin1* directory on the remote host with an IP address of 172.16.101.101:

```
Switch# copy system:running-config rcp://netadmin1@172.16.101.101/switch2-config
Write file switch-config on host 172.16.101.101? [confirm]
Building configuration... [OK]
Connected to 172.16.101.101
Switch#
```

This example shows how to store a startup configuration file on a server:

```
Switch# configure terminal
Switch(config)# ip rcmd remote-username netadmin2
Switch(config)# end
Switch# copy nvram:startup-config rcp:
Remote host []? 172.16.101.101
Name of configuration file to write [switch2-config]?
Write file switch2-config on host 172.16.101.101? [confirm]
! [OK]
```

Clearing Configuration Information

You can clear the configuration information from the startup configuration. If you reboot the switch with no startup configuration, the switch enters the setup program so that you can reconfigure the switch with new settings.

Clearing the Startup Configuration File

To clear the contents of your startup configuration, use the **erase nvram:** or the **erase startup-config** privileged EXEC command.



Caution

You cannot restore the startup configuration file after it has been deleted.

Deleting a Stored Configuration File

To delete a saved configuration from flash memory, use the **delete flash:filename** privileged EXEC command. Depending on the setting of the **file prompt** global configuration command, you might be prompted for confirmation before you delete a file. By default, the switch prompts for confirmation on destructive file operations.



Caution

You cannot restore a file after it has been deleted.

Replacing and Rolling Back Configurations

The configuration replacement and rollback feature replaces the running configuration with any saved Cisco IOS configuration file. You can use the rollback function to roll back to a previous configuration.

- [Understanding Configuration Replacement and Rollback, page 2-12](#)
- [Configuration Guidelines, page 2-13](#)
- [Replacing or Rolling Back a Configuration, page 2-14](#)

Understanding Configuration Replacement and Rollback

- [Archiving a Configuration, page 2-12](#)
- [Replacing a Configuration, page 2-13](#)
- [Rolling Back a Configuration, page 2-13](#)

Archiving a Configuration

The configuration archive provides a method to store, organize, and manage an archive of configuration files. The **configure replace** privileged EXEC command increases the configuration rollback capability. As an alternative, you can save copies of the running configuration by using the **copy running-config destination-url** privileged EXEC command, storing the replacement file either locally or remotely. However, this method lacks any automated file management. The configuration replacement and rollback feature can automatically save copies of the running configuration to the configuration archive.

The Cisco IOS configuration archive, in which the configuration files are stored and available for use with the **configure replace** command, is in any of these file systems: FTP, HTTP, RCP, TFTP.

Replacing a Configuration

The **configure replace** privileged EXEC command replaces the running configuration with any saved configuration file. When you enter the **configure replace** command, the running configuration is compared with the specified replacement configuration, and a set of configuration differences is generated. The resulting differences are used to replace the configuration. The configuration replacement operation is usually completed in no more than three passes. To prevent looping behavior, no more than five passes are performed.

You can use the **copy source-url running-config** privileged EXEC command to copy a stored configuration file to the running configuration. When using this command as an alternative to the **configure replace target-url** privileged EXEC command, note these major differences:

- The **copy source-url running-config** command is a merge operation and preserves all the commands from both the source file and the running configuration. This command does not remove commands from the running configuration that are not present in the source file. In contrast, the **configure replace target-url** command removes commands from the running configuration that are not present in the replacement file and adds commands to the running configuration that are not present.
- You can use a partial configuration file as the source file for the **copy source-url running-config** command. You must use a complete configuration file as the replacement file for the **configure replace target-url** command.

Rolling Back a Configuration

You can also use the **configure replace** command to roll back changes that were made since the previous configuration was saved. Instead of basing the rollback operation on a specific set of changes that were applied, the configuration rollback capability reverts to a specific configuration based on a saved configuration file.

If you want the configuration rollback capability, you must first save the running configuration before making any configuration changes. Then, after entering configuration changes, you can use that saved configuration file to roll back the changes by using the **configure replace target-url** command.

You can specify any saved configuration file as the rollback configuration. You are not limited to a fixed number of rollbacks, as is the case in some rollback models.

Configuration Guidelines

Follow these guidelines when configuring and performing configuration replacement and rollback:

- Make sure that the switch has free memory larger than the combined size of the two configuration files (the running configuration and the saved replacement configuration). Otherwise, the configuration replacement operation fails.
- Make sure that the switch also has sufficient free memory to execute the configuration replacement or rollback configuration commands.
- Certain configuration commands, such as those pertaining to physical components of a networking device (for example, physical interfaces), cannot be added or removed from the running configuration.
 - A configuration replacement operation cannot remove the **interface interface-id** command line from the running configuration if that interface is physically present on the device.
 - The **interface interface-id** command line cannot be added to the running configuration if that interface is not physically present on the device.

- When using the **configure replace** command, you must specify a saved configuration as the replacement configuration file for the running configuration. The replacement file must be a complete configuration generated by a Cisco IOS device (for example, a configuration generated by the **copy running-config destination-url** command).

**Note**

If you generate the replacement configuration file externally, it must comply with the format of files generated by Cisco IOS devices.

Replacing or Rolling Back a Configuration

Starting in privileged EXEC mode, follow these steps to replace the running configuration file with a saved configuration file:

	Command	Purpose
Step 1	configure replace <i>target-url</i> [list] [force] [time seconds] [nolock] Example: Switch# configure replace flash:startup-config time 120	Replaces the running configuration file with a saved configuration file. <i>target-url</i> —URL (accessible by the file system) of the saved configuration file that is to replace the running configuration. list —Displays a list of the command entries applied by the software parser during each pass of the configuration replacement operation. The total number of passes also appears. force — Replaces the running configuration file with the specified saved configuration file without prompting you for confirmation. time seconds —Specifies the time (in seconds) within which you must enter the configure confirm command to confirm replacement of the running configuration file. If you do not enter the configure confirm command within the specified time limit, the configuration replacement operation is automatically stopped. (In other words, the running configuration file is restored to the configuration that existed before you entered the configure replace command). Note You must first enable the configuration archive before you can use the time seconds command line option. nolock —Disables the locking of the running configuration file that prevents other users from changing the running configuration during a configuration replacement operation.
Step 2	configure confirm Example: Switch# configure confirm	(Optional) Confirms replacement of the running configuration with a saved configuration file. Note Use this command only if the time seconds keyword and argument of the configure replace command are specified.
Step 3	show running-config Example: Switch# show running-config	(Optional) Displays the contents of the running configuration.



Working with the Software Images

- [Image Location on the Switch, page 3-2](#)
- [File Format of Images on a Server or Cisco.com, page 3-2](#)
- [Copying Image Files Using TFTP, page 3-2](#)
- [Copying Image Files Using FTP, page 3-5](#)
- [Copying Image Files Using RCP, page 3-10](#)

Information About Software Images

You can archive (download and upload) software image files, which contain the system software, the Cisco IOS code, and the embedded Device Manager software.

You can download a switch image file from a TFTP, FTP, or RCP server to upgrade the switch software. If you do not have access to a TFTP server, you can download a software image file directly to your PC or workstation by using a web browser (HTTP) and then by using Device Manager or Cisco Network Assistant to upgrade your switch. For information about upgrading your switch by using a TFTP server or a web browser (HTTP), see the release notes.

You can replace the current image with the new one or keep the current image in flash memory after a download.

You can use the **archive download-sw /allow-feature-upgrade** privileged EXEC command to allow installation of an image with a different feature set, for example, upgrading from the universal image to the IP services feature set. You can also use the **boot auto-download-sw** global configuration command to specify a URL to use to get an image for automatic software upgrades. When you enter this command, the master switch uses this URL in case of a version mismatch.

You upload a switch image file to a TFTP, FTP, or RCP server for backup purposes. You can use this uploaded image for future downloads to the same switch or to another of the same type.

The protocol that you use depends on which type of server you are using. The FTP and RCP transport methods provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because FTP and RCP are built on and use the TCP/IP stack, which is connection-oriented.

These sections contain this configuration information:



Note

For a list of software images and the supported upgrade paths, see the release notes.

Image Location on the Switch

The Cisco IOS image is stored as a *.bin* file in a directory that shows the version number. A subdirectory contains the files needed for web management. The image is stored on the system board flash memory (flash:).

You can use the **show version** privileged EXEC command to see the software version that is currently running on your switch. In the display, check the line that begins with System image file is... . It shows the directory name in flash memory where the image is stored.

You can also use the **dir filesystem:** privileged EXEC command to see the directory names of other software images that you might have stored in flash memory. You can use the **archive download-sw /directory** privileged EXEC command to specify a directory once followed by a tar file or list of tar files to be downloaded instead of specifying complete paths with each tar file.

File Format of Images on a Server or Cisco.com

Software images on a server or downloaded from Cisco.com are in a file format, which contains these files:

- An *info* file, which serves as a table of contents for the file
- One or more subdirectories containing other images and files, such as Cisco IOS images and web management files

^T
Table 3-1 *info File Description*

Field	Description
version_suffix	Specifies the Cisco IOS image version string suffix.
version_directory	Specifies the directory where the Cisco IOS image and the HTML subdirectory are installed.
image_name	Specifies the name of the Cisco IOS image in the file.
ios_image_file_size	Specifies the Cisco IOS image size in the file, which is an approximate measure of the flash memory that the Cisco IOS image needs.
total_image_file_size	Specifies the size of all the images (the Cisco IOS image and the web management files) in the file, which is an approximate measure of the flash memory needed.
image_feature	Describes the core functionality of the image.
image_min_dram	Specifies the minimum amount of DRAM needed to run this image.
image_family	Describes the family of products on which the software can be installed.

Copying Image Files Using TFTP

You can download a switch image from a TFTP server or upload the image from the switch to a TFTP server.

You download a switch image file from a server to upgrade the switch software. You can overwrite the current image with the new one or keep the current image after a download.

You upload a switch image file to a server for backup purposes; this uploaded image can be used for future downloads to the same or another switch of the same type.

**Note**

Instead of using the **copy** privileged EXEC command or the **archive tar** privileged EXEC command, we recommend using the **archive download-sw** and **archive upload-sw** privileged EXEC commands to download and upload software image files. For switch stacks, the **archive download-sw** and **archive upload-sw** privileged EXEC commands can only be used through the stack master. Software images downloaded to the stack master are automatically downloaded to the rest of the stack members.

These sections contain this configuration information:

- [Preparing to Download or Upload an Image File Using TFTP, page 3-3](#)
- [Downloading an Image File Using TFTP, page 3-3](#)
- [Uploading an Image File Using TFTP, page 3-5](#)

Preparing to Download or Upload an Image File Using TFTP

Before you begin downloading or uploading an image file by using TFTP, do these tasks:

- Ensure that the workstation acting as the TFTP server is properly configured. On a Sun workstation, make sure that the `/etc/inetd.conf` file contains this line:

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -p -s /tftpboot
```

Make sure that the `/etc/services` file contains this line:

```
tftp 69/udp
```

**Note**

You must restart the `inetd` daemon after modifying the `/etc/inetd.conf` and `/etc/services` files. To restart the daemon, either stop the `inetd` process and restart it, or enter a **fastboot** command (on the SunOS 4.x) or a **reboot** command (on Solaris 2.x or SunOS 5.x). For more information on the TFTP daemon, see the documentation for your workstation.

- Ensure that the switch has a route to the TFTP server. The switch and the TFTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the TFTP server by using the **ping** command.
- Ensure that the image to be downloaded is in the correct directory on the TFTP server (usually `/tftpboot` on a UNIX workstation).
- For download operations, ensure that the permissions on the file are set correctly. The permission on the file should be world-read.
- Before uploading the image file, you might need to create an empty file on the TFTP server. To create an empty file, enter the **touch filename** command, where *filename* is the name of the file you will use when uploading the image to the server.
- During upload operations, if you are overwriting an existing file (including an empty file, if you had to create one) on the server, ensure that the permissions on the file are set correctly. Permissions on the file should be world-write.

Downloading an Image File Using TFTP

You can download a new image file and replace the current image or keep the current image.

Beginning in privileged EXEC mode, follow Step 1 to download a new image from a TFTP server and to overwrite the existing image. To keep the current image, follow Step 2.

Command	Purpose
Step 1 archive download-sw [/directory] /overwrite /reload tftp:[//location]/directory/image-name1.tar [image-name2.tar image-name3.tar image-name4.tar] Example: Switch# archive download-sw /overwrite /reload tftp:172.20.10.30/saved/myImage.tar	(Optional) Downloads the image files from the TFTP server to the switch, and overwrites the current image. <ul style="list-style-type: none"> • /directory—(Optional) Specifies a directory for the images. • /overwrite—Overwrites the software image in flash memory with the downloaded image. • /reload—Reloads the system after downloading the image unless the configuration has been changed and not been saved. • //location—The IP address of the TFTP server. • /directory/image-name1.tar [directory/image-name2.tar image-name3.tar image-name4.tar]—The directory (optional) and the images to download.
Step 2 archive download-sw [/directory] /leave-old-sw /reload tftp:[//location]/directory/image-name1.tar [image-name2.tar image-name3.tar image-name4.tar] Example: Switch# archive download-sw /leave-old-sw /reload tftp:172.20.10.30/saved/myImage.tar	(Optional) Downloads the images file from the TFTP server to the switch and saves the current image. <ul style="list-style-type: none"> • /directory—(Optional) Specifies a directory for the images. • /leave-old-sw—Saves the old software version after a download. • /reload—Reloads the system after downloading the image unless the configuration has been changed and not been saved. • //location—The IP address of the TFTP server. • /directory/image-name1.tar [directory/image-name2.tar image-name3.tar image-name4.tar]—The directory (optional) and the images to download.

The download algorithm verifies that the image is appropriate for the switch model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the **/overwrite** option, the download algorithm removes the existing image on the flash device whether or not it is the same as the new one, downloads the new image, and then reloads the software.



Note

If the flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

If you specify the **/leave-old-sw**, the existing files are not removed. If there is not enough space to install the new image and keep the current running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image on the system board flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT environment variable is updated to point to the newly installed image.

If you kept the old image during the download process (you specified the **/leave-old-sw** keyword), you can remove it by entering the **delete /force /recursive filesystem:/file-url** privileged EXEC command. For **filesystem**, use **flash:** for the system board flash device. For **file-url**, enter the directory name of the old image. All the files in the directory and the directory are removed.

**Caution**

For the download and upload algorithms to operate properly, do *not* rename image names.

Uploading an Image File Using TFTP

You can upload an image from the switch to a TFTP server. You can later download this image to the switch or to another switch of the same type.

Use the upload feature only if the web management pages associated with Device Manager have been installed with the existing image.

Beginning in privileged EXEC mode, follow this step to upload an image to a TFTP server:

	Command	Purpose
Step 1	archive upload-sw	Uploads the currently running switch image to the TFTP server. <ul style="list-style-type: none"> <i>//location</i>—The IP address of the TFTP server. <i>/directory/image-name.tar</i>—The directory (optional) and the name of the software image to be uploaded.
	tftp:[<i>//location</i>]/<i>directory</i>]/<i>image-name.tar</i> Example: Switch# archive upload-sw tftp:172.20.10.30/saved/myImage.tar	

The **archive upload-sw** privileged EXEC command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, and the web management files. After these files are uploaded, the upload algorithm creates the file format.

**Caution**

For the download and upload algorithms to operate properly, do *not* rename image names.

Copying Image Files Using FTP

You can download a switch image from an FTP server or upload the image from the switch to an FTP server.

You download a switch image file from a server to upgrade the switch software. You can overwrite the current image with the new one or keep the current image after a download.

You upload a switch image file to a server for backup purposes. You can use this uploaded image for future downloads to the switch or another switch of the same type.

**Note**

Instead of using the **copy** privileged EXEC command or the **archive tar** privileged EXEC command, we recommend using the **archive download-sw** and **archive upload-sw** privileged EXEC commands to download and upload software image files. For switch stacks, the **archive download-sw** and **archive upload-sw** privileged EXEC commands can only be used through the stack master. Software images downloaded to the stack master are automatically downloaded to the rest of the stack members.

These sections contain this configuration information:

- [Preparing to Download or Upload an Image File Using FTP, page 3-6](#)
- [Downloading an Image File Using FTP, page 3-7](#)
- [Uploading an Image File Using FTP, page 3-9](#)

Preparing to Download or Upload an Image File Using FTP

You can copy images files to or from an FTP server.

The FTP protocol requires a client to send a remote username and password on each FTP request to a server. When you copy an image file from the switch to a server by using FTP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **archive download-sw** or **archive upload-sw** privileged EXEC command if a username is specified.
- The username set by the **ip ftp username *username*** global configuration command if the command is configured.
- Anonymous.

The switch sends the first valid password in this list:

- The password specified in the **archive download-sw** or **archive upload-sw** privileged EXEC command if a password is specified.
- The password set by the **ip ftp password *password*** global configuration command if the command is configured.
- The switch creates a password named *username@switchname.domain*. The *username* variable is the username associated with the current session, *switchname* is the configured hostname, and *domain* is the domain of the switch.

The username and password must be associated with an account on the FTP server. If you are writing to the server, the FTP server must be properly configured to accept the FTP write request from you.

Use the **ip ftp username** and **ip ftp password** commands to specify a username and password for all copies. Include the username in the **archive download-sw** or **archive upload-sw** privileged EXEC command if you want to specify a username only for that operation.

If the server has a directory structure, the image file is written to or copied from the directory associated with the username on the server. For example, if the image file resides in the home directory of a user on the server, specify that user's name as the remote username.

Before you begin downloading or uploading an image file by using FTP, complete these tasks:

- Ensure that the switch has a route to the FTP server. The switch and the FTP server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the FTP server by using the **ping** command.
- If you are accessing the switch through the console or a Telnet session and you do not have a valid username, make sure that the current FTP username is the one that you want to use for the FTP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new FTP username by using the **ip ftp username *username*** global configuration command. This new name will be used during all archive operations. The new username is stored in NVRAM. If you are accessing the switch through a Telnet session and you have a valid username, this username is used, and you do not need to set the FTP username. Include the username in the **archive download-sw** or **archive upload-sw** privileged EXEC command if you want to specify a username for that operation only.

- When you upload an image file to the FTP server, it must be properly configured to accept the write request from the user on the switch.

For more information, see the documentation for your FTP server.

Downloading an Image File Using FTP

You can download a new image file and overwrite the current image or keep the current image.

Beginning in privileged EXEC mode, follow Steps 1 through 7 to download a new image from an FTP server and to overwrite the existing image. To keep the current image, follow Steps 1 to 6 and Step 8.

	Command	Purpose
Step 1	configure terminal Example: Switch# configure terminal	(Optional) Enters global configuration mode on the switch. This step is required only if you override the default remote username or password.
Step 2	ip ftp username <i>username</i> Example: Switch(config)# ip ftp username NetAdmin1	(Optional) Changes the default remote FTP username.
Step 3	ip ftp password <i>password</i> Example: Switch(config)# ip ftp password adminpassword	(Optional) Changes the default FTP password.
Step 4	end Example: Switch(config)# end	Returns to privileged EXEC mode.

Command	Purpose
Step 5 archive download-sw [/directory] /overwrite /reload ftp:[[/username[:password]@location]/directory] /image-name1.tar [image-name2.tar image-name3.tar image-name4.tar] Example: Switch# archive download-sw /overwrite /reload ftp:172.20.10.30/saved/myImage.tar	(Optional) Downloads the image files from the FTP server to the switch, and overwrites the current image. <ul style="list-style-type: none"> • /directory—(Optional) Specifies a directory for the images. • /overwrite—Overwrites the software image in flash memory with the downloaded image. • /reload—Reloads the system after downloading the image unless the configuration has been changed and not been saved. • //username[:password]—The username and password associated with an account on the FTP server. For more information, see the “Preparing to Download or Upload an Image File Using FTP” section on page 3-6. • @location—The IP address of the FTP server. • /directory/image-name1.tar [/directory/image-name2.tar image-name3.tar image-name4.tar]—The directory (optional) and the images to download.
Step 6 archive download-sw [/directory] /leave-old-sw /reload ftp:[[/username[:password]@location]/directory] /image-name1.tar [image-name2.tar image-name3.tar image-name4.tar] Example: Switch# archive download-sw /leave-old-sw /reload ftp:172.20.10.30/saved/myImage.tar	(Optional) Downloads the image files from the FTP server to the switch and saves the current image. <ul style="list-style-type: none"> • /directory—(Optional) Specifies a directory for the images. • /leave-old-sw—Saves the old software version after a download. • /reload—Reloads the system after downloading the image unless the configuration has been changed and not been saved. • //username[:password]—The username and password associated with an account on the FTP server. For more information, see the “Preparing to Download or Upload an Image File Using FTP” section on page 3-6. • @location—The IP address of the TFTP server. • /directory/image-name1.tar [/directory/image-name2.tar image-name3.tar image-name4.tar]—The directory (optional) and the images to download.

The download algorithm verifies that the image is appropriate for the switch model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the **/overwrite** option, the download algorithm removes the existing image on the flash device, whether or not it is the same as the new one, downloads the new image, and then reloads the software.


Note

If the flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

If you specify the **/leave-old-sw** option, the existing files are not removed. If there is not enough space to install the new image and keep the running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image onto the system board flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT environment variable is updated to point to the newly installed image.

If you kept the old image during the download process (you specified the **/leave-old-sw** keyword), you can remove it by entering the **delete /force /recursive filesystem:/file-url** privileged EXEC command. For *filesystem*, use **flash:** for the system board flash device. For *file-url*, enter the directory name of the old software image. All the files in the directory and the directory are removed.

**Caution**

For the download and upload algorithms to operate properly, do *not* rename image names.

Uploading an Image File Using FTP

You can upload an image from the switch to an FTP server. You can later download this image to the same switch or to another switch of the same type.

Use the upload feature only if the web management pages associated with Device Manager have been installed with the existing image.

Beginning in privileged EXEC mode, follow these steps to upload an image to an FTP server:

	Command	Purpose
Step 1	configure terminal Example: Switch# configure terminal	(Optional) Enters global configuration mode on the switch. This step is required only if you override the default remote username or password.
Step 2	ip ftp username <i>username</i> Example: Switch(config)# ip ftp username NetAdmin1	(Optional) Changes the default remote FTP username.
Step 3	ip ftp password <i>password</i> Example: Switch(config)# ip ftp password adminpassword	(Optional) Changes the default FTP password.

	Command	Purpose
Step 4	end	Returns to privileged EXEC mode.
	Example: Switch(config)# end	
Step 5	archive upload-sw ftp:[[/[username[:password]@]location]/directory]/ image-name.tar. Example: Switch# archive upload-sw ftp://172.20.10.30/myImage.tar	Uploads the currently running switch image to the FTP server. <ul style="list-style-type: none"> • <i>//username:password</i>—The username and password associated with an account on the FTP server. For more information, see the “Preparing to Download or Upload an Image File Using FTP” section on page 3-6. • <i>@location</i>—The IP address of the FTP server. • <i>/directory/image-name.tar</i>—The directory (optional) and the name of the software image to be uploaded.

The **archive upload-sw** command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, and the web management files. After these files are uploaded, the upload algorithm creates the file format.



Caution For the download and upload algorithms to operate properly, do *not* rename image names.

Copying Image Files Using RCP

You can download a switch image from an RCP server or upload the image from the switch to an RCP server.

You download a switch image file from a server to upgrade the switch software. You can overwrite the current image with the new one or keep the current image after a download.

You upload a switch image file to a server for backup purposes. You can use this uploaded image for future downloads to the same switch or another of the same type.



Note Instead of using the **copy** privileged EXEC command or the **archive tar** privileged EXEC command, we recommend using the **archive download-sw** and **archive upload-sw** privileged EXEC commands to download and upload software image files. For switch stacks, the **archive download-sw** and **archive upload-sw** privileged EXEC commands can only be used through the stack master. Software images downloaded to the stack master are automatically downloaded to the rest of the stack members.

These sections contain this configuration information:

- [Preparing to Download or Upload an Image File Using RCP, page 3-11](#)
- [Downloading an Image File Using RCP, page 3-12](#)
- [Uploading an Image File Using RCP, page 3-13](#)

Preparing to Download or Upload an Image File Using RCP

RCP provides another method of downloading and uploading image files between remote hosts and the switch. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, RCP uses TCP, which is connection-oriented.

To use RCP to copy files, the server from or to which you will be copying files must support RCP. The RCP copy commands rely on the rsh server (or daemon) on the remote system. To copy files by using RCP, you do not need to create a server for file distribution as you do with TFTP. You only need to have access to a server that supports the remote shell (rsh). (Most UNIX systems support rsh.) Because you are copying a file from one place to another, you must have read permission on the source file and write permission on the destination file. If the destination file does not exist, RCP creates it for you.

RCP requires a client to send a remote username on each RCP request to a server. When you copy an image from the switch to a server by using RCP, the Cisco IOS software sends the first valid username in this list:

- The username specified in the **archive download-sw** or **archive upload-sw** privileged EXEC command if a username is specified.
- The username set by the **ip rcmd remote-username** *username* global configuration command if the command is entered.
- The remote username associated with the current TTY (terminal) process. For example, if the user is connected to the router through Telnet and was authenticated through the **username** command, the switch software sends the Telnet username as the remote username.
- The switch hostname.

For the RCP copy request to execute successfully, an account must be defined on the network server for the remote username. If the server has a directory structure, the image file is written to or copied from the directory associated with the remote username on the server. For example, if the image file resides in the home directory of a user on the server, specify that user's name as the remote username.

Before you begin downloading or uploading an image file by using RCP, do these tasks:

- Ensure that the workstation acting as the RCP server supports the remote shell (rsh).
- Ensure that the switch has a route to the RCP server. The switch and the server must be in the same subnetwork if you do not have a router to route traffic between subnets. Check connectivity to the RCP server by using the **ping** command.
- If you are accessing the switch through the console or a Telnet session and you do not have a valid username, make sure that the current RCP username is the one that you want to use for the RCP download. You can enter the **show users** privileged EXEC command to view the valid username. If you do not want to use this username, create a new RCP username by using the **ip rcmd remote-username** *username* global configuration command to be used during all archive operations. The new username is stored in NVRAM. If you are accessing the switch through a Telnet session and you have a valid username, this username is used, and there is no need to set the RCP username. Include the username in the **archive download-sw** or **archive upload-sw** privileged EXEC command if you want to specify a username only for that operation.
- When you upload an image to the RCP to the server, it must be properly configured to accept the RCP write request from the user on the switch. For UNIX systems, you must add an entry to the .rhosts file for the remote user on the RCP server. For example, suppose the switch contains these configuration lines:

```
hostname Switch1
ip rcmd remote-username User0
```

If the switch IP address translates to *Switch1.company.com*, the *.rhosts* file for User0 on the RCP server should contain this line:

```
Switch1.company.com Switch1
```

For more information, see the documentation for your RCP server.

Downloading an Image File Using RCP

You can download a new image file and replace or keep the current image.

Beginning in privileged EXEC mode, follow Steps 1 through 6 to download a new image from an RCP server and overwrite the existing image. To keep the current image, go to Step 6.

	Command	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).
Step 2	ip rcmd remote-username <i>username</i> Example: Switch(config)# ip rcmd remote-username netadmin1	(Optional) Specifies the remote username.
Step 3	end Example: Switch(config)# end	Returns to privileged EXEC mode.
Step 4	archive download-sw /overwrite /reload rcp:[<i>[[username@location]/directory]/image-name1.tar [image-name2.tar image-name3.tar image-name4.tar]</i> Example: Switch# archive download-sw /overwrite /reload rcp://172.20.10.30/saved/myImage.tar	Downloads the images file from the RCP server to the switch and overwrites the current image. <ul style="list-style-type: none">• /overwrite— Overwrites the software image in flash memory with the downloaded image.• /reload— Reloads the system after downloading the image unless the configuration has been changed and not been saved.• //username—The username associated with an account on the network server. For more information, see the “Preparing to Download or Upload an Image File Using RCP” section on page 3-11.• @location—The IP address of the RCP server.• /directory/image-name1.tar [/directory/image-name2.tar image-name3.tar image-name4.tar]—The directory (optional) and the images to download.

Command	Purpose
Step 5 archive download-sw /leave-old-sw /reload rcp:[[/username@location]/directory]/image -name1.tar [image-name2.tar image-name3.tar image-name4.tar] Example: Switch# archive download-sw /leave-old-sw rcp://172.20.10.30/myNewImage.tar	Downloads the images file from the RCP server to the switch and saves the current image. <ul style="list-style-type: none"> • /leave-old-sw—Saves the old software version after a download. • /reload—Reloads the system after downloading the image unless the configuration has been changed and not been saved. • //username—The username associated with an account on the network server. For more information, see the “Preparing to Download or Upload an Image File Using RCP” section on page 3-11. • @location—The IP address of the RCP server. • /directory/image-name1.tar [/directory/image-name2.tar image-name3.tar image-name4.tar]—The directory (optional) and the images to download.

The download algorithm verifies that the image is appropriate for the switch model and that enough DRAM is present, or it aborts the process and reports an error. If you specify the **/overwrite** option, the download algorithm removes the existing image on the flash device whether or not it is the same as the new one, downloads the new image, and then reloads the software.

**Note**

If the flash device has sufficient space to hold two images and you want to overwrite one of these images with the same version, you must specify the **/overwrite** option.

If you specify the **/leave-old-sw**, the existing files are not removed. If there is not enough room to install the new image and keep the running image, the download process stops, and an error message is displayed.

The algorithm installs the downloaded image onto the system board flash device (flash:). The image is placed into a new directory named with the software version string, and the BOOT environment variable is updated to point to the newly installed image.

If you kept the old software during the download process (you specified the **/leave-old-sw** keyword), you can remove it by entering the **delete /force /recursive filesystem:/file-url** privileged EXEC command. For *filesystem*, use **flash:** for the system board flash device. For *file-url*, enter the directory name of the old software image. All the files in the directory and the directory are removed.

**Caution**

For the download and upload algorithms to operate properly, do *not* rename image names.

Uploading an Image File Using RCP

You can upload an image from the switch to an RCP server. You can later download this image to the same switch or to another switch of the same type.

The upload feature should be used only if the web management pages associated with Device Manager have been installed with the existing image.

Beginning in privileged EXEC mode, follow these steps to upload an image to an RCP server:

	Command	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode. This step is required only if you override the default remote username (see Steps 4 and 5).
Step 2	ip rcmd remote-username <i>username</i>	(Optional) Specifies the remote username.
Step 3	end	Returns to privileged EXEC mode.
Step 4	archive upload-sw rcp: [[[// <i>[username@location]/directory/</i> image-name <i>.tar</i>] Example: Switch# archive upload-sw rcp:	Uploads the currently running switch image to the network server. <ul style="list-style-type: none"> • <i>//username</i>—The username associated with an account on the network server. For more information, see the “Preparing to Download or Upload an Image File Using RCP” section on page 3-11. • <i>@location</i>—The IP address of the RCP server. • <i>/directory/image-name1.tar</i> [<i>/directory/image-name2.tar image-name3.tar image-name4.tar</i>]—The directory (optional) and the images to download.

The **archive upload-sw** privileged EXEC command builds an image file on the server by uploading these files in order: info, the Cisco IOS image, and the web management files. After these files are uploaded, the upload algorithm creates the file format.



Caution

For the download and upload algorithms to operate properly, do *not* rename image names.